Deutscher Bundestag **Drucksache 18/9616**

18. Wahlperiode 06.09.2016

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Volker Beck (Köln), Katja Keul, Renate Künast, Monika Lazar, Irene Mihalic, Özcan Mutlu, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Im Internet offen abrufbare NSA-Hackingwerkzeuge

Im Verlauf des 13./14. August 2016 wurden überraschend auf der Software-Tauschplattform GitHub 300 Megabyte anspruchsvolle Programme angeboten, mit denen unter anderem das gezielte Hacking von weit verbreiteten kommerziellen Firewalls von Anbietern wie CISCO und Fortinet, von Routern, Betriebssysteme etc. möglich sein soll. Bei den erkennbar nur einen Teil eines Gesamtbestandes darstellenden Programmen soll es sich um Entwicklungen der der NSA-Elitehackergruppe TAO zugeordneten Equation Group handeln, deren Echtheit und Funktionsfähigkeit inzwischen von Experten allgemein bestätigt wird (vgl. „Hacker erbeuteten offenbar NSA-Software“, SPIEGEL ONLINE vom 17. August 2016). Zu der Veröffentlichung der zwischenzeitlich am ursprünglichen Ort nicht mehr verfügbaren, aber vielfach an anderer Stelle gespiegelten Dokumenten und Programmen bekannte sich eine Gruppe mit Namen Shadow Brokers. Während zunächst spekuliert wurde, ob die NSA selbst gehackt worden sein könnte, schätzen einige Experten die angebotenen Programme mittlerweile als das Leak eines Insiders ein, so dass die Möglichkeit diskutiert wird, ob nach Edward Snowden eine weitere Person aus dem weiten Beschäftigtenkreis der NSA gezielt Informationen an die Öffentlichkeit gegeben haben könnte (vgl. beispielsweise Erich Möchel „Der aktuelle NSA-„Hack“ war ein Insiderjob, abrufbar unter http://fm4.orf.at/stories/1772666/).

Nach Angaben unabhängiger Experten stellen die offenbar unter NSA-internen Codenamen veröffentlichten Hacking-Werkzeuge wie Epicbanana, Buzzdirection und Egregiousblunder eine reale und ernstzunehmende Bedrohung für die Sicherheit von Regierungs- und Unternehmensnetzwerken weltweit dar (vgl. Ellen Nakashima „Powerful NSA hacking tools have been revealed online, abrufbar unter www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html).

Die Plattform WikiLeaks hatte in der Zwischenzeit angekündigt, über eine eigene Kopie des veröffentlichten Pakets von Hacking-Werkzeugen zu verfügen, welches ebenfalls zu gegebener Zeit veröffentlicht werden soll. Bisher hat diese Veröffentlichung jedoch noch nicht stattgefunden.

Wir fragen die Bundesregierung:

1. Wann hat die Bundesregierung (einschließlich die ihr nachgeordneten Behörden) erstmalig von der Veröffentlichung der Hacking-Werkzeuge Kenntnis erhalten?
2. Wie bewertet die Bundesregierung die Echtheit der angebotenen Hacking-Werkzeuge, und worauf stützt sich ihr Urteil?
3. In welchem Umfang waren bzw. sind bundesdeutsche Behörden und Unternehmen von den offengelegten Schwachstellen, beispielsweise von CISCO- und Fortinet Netzwerktechnik (siehe hierzu im Einzelnen http://blogs.cisco.com/security/shadow-brokers), betroffen (bitte nach Behörden bzw. Ministerien je gesondert ausführen), und wurden zwischenzeitlich die erforderlichen Gegenmaßnahmen getroffen?
4. Was wurde von der Bundesregierung bzw. den zuständigen Bundesbehörden wann veranlasst, um etwaigen Schaden von Regierungs- als auch Unternehmensnetzwerken der Bundesrepublik Deutschland abzuwenden?
5. Wie bewertet die Bundesregierung die Frage, ob es sich um ein Hack einer der NSA nahestehenden bzw. der NSA zugehörigen Gruppe (z. B. der sogenannten Equation Group) oder die Veröffentlichung eines möglichen NSA-Beschäftigten selbst handeln könnte, und welche Erkenntnisse liegen ihr (oder ihr nachgeordnete Behörden) hierzu vor?
6. Wie bewertet die Bundesregierung die Frage, ob es sich um ein Hack einer der russischen Regierung nahestehenden Gruppe handeln könnte, und welche Erkenntnisse liegen ihr (oder ihr nachgeordnete Behörden) hierzu vor?
7. Hat die Bundesregierung (oder ihr nachgeordnete Behörden) Kenntnisse bezüglich der Frage, von wann die entwendete Software ist, und ob die entsprechenden Sicherheitslücken mittlerweile geschlossen wurden?

   Wenn ja, welche Sicherheitslücken wurden zwischenzeitlich geschlossen, und welche bestehen weiterhin?
8. Hat die Bundesregierung (oder ihr nachgeordnete Behörden) Kenntnisse bezüglich der Frage, ob es sich um einen gezielten Hack oder eventuell eher um einen „Zufallsfund“ auf einem von der „Equation Group“ oder anderen Gruppe verwendeten Command-and-Control-Server handelt?

   Wenn ja, welche?
9. Welche Erkenntnisse hat die Bundesregierung (oder ihr nachgeordnete Behörden) zu Verbindungen von den nun veröffentlichten Dokumenten und den Dokumenten aus dem Umfeld Edward Snowdens, und welche Rückschlüsse lassen diese Erkenntnisse aus Sicht der Bundesregierung auf die jeweilige Echtheit der veröffentlichten Dokumente zu?
10. Unabhängig von der Frage der Herkunft und Verantwortung für die Erstellung der Hacking-Werkzeuge, hält die Bundesregierung es für die Aufgabe auch bundesdeutscher Behörden (etwa die geplante ZITIS), kommerzielle Netzwerkelemente wie beispielsweise die betroffenen, weithin im Einsatz befindlichen CISCO- und und Fortinet-Produkte, Firewall-Programme, Router, Betriebssysteme etc. gezielt auf Schwachstellen zu analysieren und für den Angriff auf Netzwerke derartige Instrumente und das Wissen über Schwachstellen vorzuhalten?

11. Teilt die Bundesregierung, auch angesichts der jetzigen Veröffentlichungen, die Ansicht der Fragesteller, dass es dringend angeraten ist, Schwachstellen, sobald sie bekannt sind, statt sie bewusst offen zu halten, um sie ggf. zu einem späteren Zeitpunkt nutzen zu können, umgehend zu schließen, auch, um zu verhindern, dass diese Dritten offenstehen und ggf. missbraucht werden können?

12. Wird sich die Bundesregierung, wie dies beispielsweise in einem Entschließungsantrag der fragestellenden Fraktion zu der dritten Beratung des Gesetzentwurfs der Bundesregierung eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) auf Bundestagsdrucksache 18/5127 im Juni 2015 forderte, für eine grundsätzliche Pflicht zur unverzüglichen Veröffentlichung von Wissen über Sicherheitslücken einsetzen?

13. Wird die Bundesregierung, wie dies in der in Frage 12 Erwähnung findenden Initiative gefordert wird, dafür Sorge tragen, dass, auch um eine Beförderung des Schwarzmarktes für Sicherheitslücken, welche die Integrität digitaler Infrastrukturen gefährden, der staatliche Aufkauf und die Zurückhaltung bzw. Nichtveröffentlichung von Wissen über Sicherheitslücken, gesetzlich verboten wird?

    Wenn ja, wann ist mit der Vorlage zu rechnen?

    Falls nein, warum nicht?

14. Sieht die Bundesregierung den Ankauf und die Zurückhaltung bzw. Nichtveröffentlichung von Wissen über Sicherheitslücken durch staatliche Stellen als vereinbar mit ihrem Ziel, die IT-Sicherheit zu erhöhen, an oder teilt die Bundesregierung die Ansicht der Fragesteller, dass beides nicht miteinander in Einklang zu bringen ist?

15. Verfügt die Bundesregierung oder ihr nachgeordnete Behörden inzwischen über Kopien der online angebotenen Hacking-Werkzeuge, und wenn nein, auf welche Weise wurde Vorsorge getroffen (etwa durch Ansprache anderer betroffener Staaten; Kontakt mit den USA, der NSA etc.), dass diese Werkzeuge nicht gegen Stellen in und gegen Institutionen der Bundesrepublik Deutschland eingesetzt werden können?

16. Sind Regierungsstellen bzw. Teile von Regierungsnetzwerken von den von CISCO benannten Sicherheitslücken (Exploits) oder anderen Schwachstellen, z. B. für die Umgehung von gängigen Firewall-Programmen, zur Infiltrierung von Routern und/oder Betriebssystemen, betroffen, wenn ja, in welchem bezifferbaren Umfang, und konnten diese Lücken inzwischen geschlossen werden?

17. Wurde zwischenzeitlich der zur Koordination mit der Wirtschaft geschaffene Cybersicherheitsrat mit diesem Vorfall befasst, und wenn ja, wann, und mit welcher Zielrichtung?

18. Wann war das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstmalig mit diesem Vorgang befasst, und was hat es hierzu zwischenzeitlich veranlasst?

19. Gibt der Vorfall der Bundesregierung Anlass, ihre Bewertung der Vorteile und Risiken der Neugründung der sogenannten ZITIS-Behörde zu überdenken, welche selbst zum ausgewählten Ziel von Angriffen werden dürfte, die bei Erfolg gravierende Risiken für die nationalen Kommunikationsinfrastrukturen als auch für die Betriebs- und Geschäftsgeheimnisse von Unternehmen der Wirtschaft nach sich ziehen?

Berlin, den 6. September 2016

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333